1/9/1
DIALOG(R)File 351:Derwent WPI

013508356 **Image available**
WPI Acc No: 2000-680302/*200067*
XRPX Acc No: N00-503596

Methods for anonymisation of sensitive data within data stream by anonymisation of sensitive data field and qualification of anonymised sensitive data field within data stream by start and stop signs

Patent Assignee: LOK LOMBARDKASSE AG (LOKL-N)
Inventor: NEHL R
Number of Countries: 022 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 19911176	A1	20000921	DE 1011176	A	19990312	200067	B
WO 200056005	A2	20000921	WO 2000DE586	A	20000302	200067	
EP 1163776	A2	20011219	EP 2000916771	A	20000302	200206	
			WO 2000DE586	A	20000302		
JP 2002539545	W	20021119	JP 2000605337	A	20000302	200281	
			WO 2000DE586	A	20000302		

Priority Applications (No Type Date): DE 1011176 A 19990312
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 19911176	A1		10	H04L-009/00	
WO 200056005	A2	G		H04L-009/00	
Designated States (National): CA JP US					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
EP 1163776	A2	G		H04L-029/06	Based on patent WO 200056005
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
JP 2002539545	W		23	G06F-012/00	Based on patent WO 200056005

Abstract (Basic): *DE 19911176* A1

NOVELTY - The method involves anonymisation of the sensitive data field and qualification of the anonymised sensitive data field within the data stream by start and stop signs.

DETAILED DESCRIPTION - The data field for anonymizing is first checked for its capacity. It has to be ensured that after the encoding, there is still sufficient place within the fixed field width in order to insert a start and a stop sign and a used key information.

USE - In database information of the long-term storage where such collections of information is regarded as an essential material by organizations, in which the access is permitted only for authorized users.

ADVANTAGE - The access to a database excludes certain data from the viewing within this database destroying the assignment of the excluded data to the remaining data. The database should be able for working on the unprotected data without the access to the protected data.

DESCRIPTION OF DRAWING(S) - The drawing shows an stages of encoding according to the present invention.

pp; 10 DwgNo 5/5

Title Terms: METHOD; SENSITIVE; DATA; DATA; STREAM; SENSITIVE; DATA; FIELD; QUALIFY; SENSITIVE; DATA; FIELD; DATA; STREAM; START; STOP; SIGN
Derwent Class: T01; W01
International Patent Class (Main): G06F-012/00; H04L-009/00; H04L-029/06
International Patent Class (Additional): G06F-012/14; G06F-017/30; H04L-009/36
File Segment: EPI
Manual Codes (EPI/S-X): T01-H01C2; T01-J05B; W01-A05; W01-A05A

02P17067

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 199 11 176 A 1**

(51) Int. Cl.[7]:
H 04 L 9/00
G 06 F 12/14
G 06 F 17/30

(21) Aktenzeichen: 199 11 176.6
(22) Anmeldetag: 12. 3. 1999
(43) Offenlegungstag: 21. 9. 2000

(71) Anmelder:
LOK Lombardkasse AG, 60323 Frankfurt, DE

(74) Vertreter:
Feddersen Laule Scherzberg & Ohle Hansen Ewerwahn, 20354 Hamburg

(72) Erfinder:
Nehl, Roland, Dr., 35789 Weilmünster, DE

(56) Entgegenhaltungen:

US	53 03 303
US	50 86 467
JP	10-49 048 A

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Anonymisierungsverfahren

(57) Die Erfindung betrifft ein Verfahren zur Anonymisierung sensibler Daten innerhalb eines Datenstroms. Erfindungsgemäß wird ein Verfahren vorgeschlagen, das die Schritte Komprimierung des sensiblen Datenfeldes, Anonymisierung des sensiblen Datenfeldes und Kennzeichnung des anonymisierten sensiblen Datenfeldes innerhalb des Datenstroms durch Start- und Stopzeichen umfaßt.

DE 199 11 176 A 1

DE 199 11 176 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zur Anonymisierung sensibler Daten innerhalb eines Datenstroms.

In Datenbanken werden Informationen zur langfristigen Aufbewahrung gespeichert. Der Wert solcher Informationssammlungen wird als wesentliches Gut von Organisationen angesehen. Aufgrund der Sensitivität wird im allgemeinen der Zugriff auf Datenbanken beschränkt, d. h. daß der Zugriff nur für autorisierte Anwender gemäß deren Rechteprofil möglich ist. In einem Rechteprofil kann festgelegt werden, wer auf welche Daten mit welchen Modi (z. B. lesend, schreibend) zugreifen kann. Ein gängiges Beispiel ist, daß nicht jeder Mitarbeiter eines Unternehmens Personaldaten einsehen kann. Auch gemäß dem "Need to know"-Prinzip können Mitarbeiter ausschließlich die Informationen einsehen, die sie zur Ausübung ihrer dienstlichen Tätigkeiten benötigen. Alle weiteren Informationen sind gesperrt. Für die Vergabe der Zugriffsrechte ist ein Administrator zuständig, von dessen Zuverlässigkeit der Datenschutz im wesentlichen abhängt.

Zur Datensicherung werden häufig Anonymisierungsverfahren eingesetzt, die diejenigen Daten, auf die kein Zugriff erfolgen soll, anonymisieren. Solche Verfahren werden insbesondere verwendet, wenn Daten einer Datenbank in Form eines Datenstroms übermittelt werden sollen, wobei sichergestellt werden muß, daß auf dem Übermittlungsweg kein unberechtigter Zugriff auf die Daten erfolgt. Ein Anwendungsbeispiel hierfür ist die Versendung eines Datenstroms per E-Mail. Dabei haben Sender und Empfänger volle Zugriffsrechte auf alle in der Datenbank enthaltenen Daten. Die Daten werden vor Absendung verschlüsselt, so daß Angreifer innerhalb des Internets keinen Zugriff auf die Daten nehmen können. Der Empfänger entschlüsselt die Daten und kann vollständigen Zugriff darauf nehmen.

Bei den bekannten Verfahren zum Schutz von Datenbanken wird die Autorisierung und Rechteprüfung typischerweise am Datenbank-Front End realisiert. Dies trifft z. B. für DB2™ von IBM zu. Wird ein höheres Niveau bzgl. des Zugriffsschutzes gefordert, so gibt es kommerzielle Produkte, wie z. B. RACF™ (Ressource Access Control Facility) von IBM. Die Zugriffskontrolle wird jedoch auch hier von einem Administrator kontrolliert.

Eine klassische Situation, in der die herkömmlichen Verfahren unzureichend sind, ist eine Outsourcer/Insourcer-Beziehung. Ein Outsourcer läßt bestimmte Dienste durch einen Insourcer erbringen und übergibt dem Insourcer alle dafür notwendigen Daten, die beim Insourcer in einer Datenbank gespeichert werden. Wenn der Outsourcer aus Datenschutzgründen oder aus Gründen des Kundenschutzes die Weitergabe von kundenidentifizierenden Daten eigenständig kontrollieren will, wird mit den bekannten Anonymisierungsverfahren entweder der Zugriff auf die gesamte Datenbank unterbunden oder die selektive Kontrolle über den Zugriff auf bestimmte Daten einem Administrator unterstellt, der im dem Hause des Insourcers angesiedelt ist. Grundsätzlich wäre der Zugriff somit auch auf sensible Daten möglich.

Es ist Aufgabe der vorliegenden Erfindung, ein Verfahren zur Verfügung zu stellen, das den Zugriff auf eine Datenbank ermöglicht, dabei aber bestimmte Daten innerhalb dieser Datenbank vom Zugriff ausschließt, ohne die Zuordnung der ausgeschlossenen Daten zu den restlichen Daten zu zerstören. Die Datenbank soll zur Bearbeitung der nicht geschützten Daten in dritte Hände gegeben werden können, ohne daß die Zugriffskontrolle auf die geschützten Daten aus der Hand gegeben wird.

Erfindungsgemäß wird ein Verfahren zur Anonymisierung sensibler Daten innerhalb eines Datenstroms mit folgenden Schritten vorgeschlagen:

a) Anonymisierung des sensiblen Datenfelds;
b) Kennzeichnung des anonymisierten sensiblen Datenfelds innerhalb des Datenstroms durch Start- und Stoppzeichen.

Erfindungsgemäß werden die sensiblen Daten innerhalb einer Datenbank selektiv anonymisiert. Die anonymisierten Datenfelder werden mit einem Start- und einem Stoppzeichen versehen, um sie für die spätere Deanonymisierung kenntlich zu machen.

Das erfindungsgemäße Verfahren kann insbesondere eingesetzt werden, wenn ein Datenbanknutzer Daten in einer Datenbank ablegt, und Teile der Daten durch einen Datenbankbetreiber bearbeitet werden sollen. Während der Datenbanknutzer autorisiert ist, sämtliche Daten zu lesen, sollen sensible Daten, wie z. B. kundenidentifizierende Informationen, für den Datenbankbetreiber anonymisiert und nicht deanonymisierbar sein. Die Anonymisierungsinformation verbleibt beim Datenbanknutzer. Die nicht anonymisierten Daten können vom Datenbankbetreiber ausgewertet und bearbeitet werden. Die Zuordnung der Daten zueinander bleibt erhalten.

Die sensiblen Daten können beispielsweise kundenidentifizierende Informationen sein, wobei die dem Kunden zugeordneten Daten zwecks statistischer Auswertung lesbar sein sollen. Die Datenbank kann mit dem erfindungsgemäßen Anonymisierungsverfahren partiell anonymisiert und an Dritte zur statistischen Auswertung und Bearbeitung weitergegeben werden. Die kundenidentifizierenden Daten sind für den Dritten nicht lesbar. Die Kontrolle darüber, welche Zugriffsrechte für welche Personen bestehen, verbleibt beim Datenbanknutzer. Die Zuordnung zwischen den bearbeiteten Daten und den jeweiligen anonymisierten Daten, wie Kundennamen, bleibt erhalten. Nach Rückgabe der ausgewerteten oder bearbeiteten Datenbank an den Datenbanknutzer kann dieser die Deanonymisierung vornehmen und die vollständige, bearbeitete Datenbank nutzen.

Das erfindungsgemäße Verfahren läßt sich insbesondere auch dann vorteilhaft anwenden, wenn die sensiblen Datenfelder eine vorgegebene Feldlänge aufweisen. Es versteht sich aber von selbst, daß das Verfahren ohne Einschränkung auch bei unbegrenzten Feldlängen entsprechend anwendbar ist. Auch wenn sich die nachfolgenden Ausführungen vermehrt auf sensible Datenfelder vorgegebener Feldlänge beziehen, ist dies nicht einschränkend zu verstehen.

Vorteilhaft kann vor der Anonymisierung des sensiblen Datenfeldes eine Komprimierung der Daten vorgenommen werden. Im Falle der vollständigen Füllung des Datenfeldes wird auf diesem Wege Platz für die Hinzufügung von Start- und Stoppzeichen zur Kennzeichnung des anonymisierten Datenfeldes geschaffen. Die Kennzeichnung ist notwendig zur späteren Deanonymisierung des Datenfeldes.

Ist das Datenfeld ohnehin nicht vollständig gefüllt, oder sind die Daten durch die Komprimierung soweit komprimiert, daß noch Platz im Datenfeld verbleibt, kann das Datenfeld vor der Anonymisierung durch Füllzeichen aufgefüllt werden.

Es stehen insbesondere zwei Möglichkeiten zur Anonymisierung des Datenfeldes zur Verfügung, nämlich die Pseudonymisierung und die Verschlüsselung.

Ist das Datenfeld vollständig gefüllt, wird vorzugsweise eine Pseudonymisierung vorgenommen. Dabei muß die Länge des verwendeten Pseudonyms so gewählt werden, daß im Datenfeld nach der Pseudonymisierung Platz für Start- und Stoppzeichen verbleibt.

Verbleibt innerhalb des Datenfeldes noch Platz, so wird

das Datenfeld vorzugsweise durch Füllzeichen, insbesondere mit zufälligen Werten, zumindest teilweise aufgefüllt und anschließend verschlüsselt.

Die Auffüllung des Feldes mit zufälligen Werten sichert die Auflösung von Isonomien. Beispielsweise ist es erforderlich, daß häufig auftretende Namen, wie im deutschen Sprachraum Müller, Meier usw. verschieden verschlüsselt werden, damit über eine Analyse der Häufigkeit der Daten keine Rückschlüsse auf die Daten gezogen werden kann. Dies wird mit der Auffüllung des Datenfeldes durch zufällige Werte und anschließende Verschlüsselung erreicht.

In einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens werden im verschlüsselten Datenfeld auch Informationen über den zur Verschlüsselung verwendeten Schlüssel abgelegt. Diese Schlüsselinformationen dienen dem Datenbanknutzer dazu, die verschlüsselten Daten entschlüsseln zu können. Auf diesem Wege können verschiedene Schlüssel zur Verschlüsselung der Daten verwendet werden, wobei jeweils innerhalb des Feldes die entsprechenden Schlüsselinformationen zur Identifizierung des Schlüssels abgelegt werden. Es versteht sich von selbst, daß der Füllgrad des Feldes so beschaffen oder durch Datenkompression erzeugt werden muß, daß Platz zum Ablegen einer Schlüsselinformation verbleibt.

Das Erkennen, welche Daten zu ver- bzw. entschlüsseln sind, kann durch eindeutige Kennzeichnung durch sogenannte Start- und Stoppzeichen, wie z. B. "{" und "}" realisiert werden. Diese Start- und Stoppzeichen dürfen im betroffenen System außer zur Kennzeichnung verschlüsselter Daten nicht verwendet werden. Dieser Ansatz hat den Vorteil, daß er unabhängig von den Anwendungen, die auf den Daten operieren, ist.

Gibt es im betrachteten System kein einziges eindeutiges Startzeichen, kann eine Menge von Startzeichen verwendet werden. Gleiches gilt für das Stoppzeichen. Im einfachsten Fall könnte die Menge der Startzeichen aus einem Zeichen bestehen, welches mit dem Stoppzeichen identisch ist. Dies hat allerdings wiederum den Nachteil, daß eine Synchronisierung in einem Fehlerfall alleine aufgrund der Kenntnis von Start- und Stoppzeichen nicht mehr möglich ist.

Das erfindungsgemäße Verfahren wird im folgenden anhand von verschiedenen Beispielen mit Bezug auf die beigefügten Abbildungen näher erläutert:

Fig. 1 zeigt die Kennzeichnung von sensiblen, zu anonymisierenden Daten;

Fig. 2 zeigt das Ablaufschema einer Ver- bzw. Entschlüsselung;

Fig. 3 zeigt den Ablauf eines Verschlüsselungsprozesses;

Fig. 4 zeigt die Struktur eines verschlüsselten Datenfeldes;

Fig. 5 zeigt den Ablauf eines Entschlüsselungsprozesses.

Das Anonymisierungsverfahren soll folgende Anforderungen erfüllen:

1. Häufig vorkommende Daten (z. B. die häufig auftretenden Namen Müller, Meier usw. im deutschen Sprachraum) sollen verschieden verschlüsselt werden. Dadurch soll verhindert werden, daß über die Analyse der Häufigkeit von Daten Schlüsse auf die Daten selbst gezogen werden können. Die Isonomien der Daten sollen aufgelöst werden.
2. Die Länge eines zu verschlüsselndes Datenfelds ist durch eine fixe, maximale Länge beschränkt, die im wesentlichen durch das Datenbank-Design vorgegeben ist. Feldtypen, z. B. numerisch oder alphanumerisch dürfen nicht verändert werden. Diese Anforderung ermöglicht eine nachträgliche Integration des Verfahrens, ohne daß ein Betreiber eines Datenbanksystems seine Anwendungen zur Verarbeitung der Daten verändern muß.
3. Jedes verschlüsselte Datenfeld enthält alle Informationen außer Schlüssel und systemweite Parameter zur Entschlüsselung. Ein autarkes Verarbeiten jedes Datenfeldes ist deshalb möglich.

Die vorgenannten drei Eigenschaften sollen von dem gewählten Anonymisierungsverfahren gleichzeitig erfüllt werden.

Zur Durchführung des Verfahrens wird das zu anonymisierende Datenfeld zunächst auf seinen Füllgrad hin überprüft. Es muß sichergestellt werden, daß nach der Verschlüsselung noch genügend Platz innerhalb der vorgegebenen festen Datenfeldlänge verbleibt, um ein Start- sowie ein Stoppzeichen und eine Information für den verwendeten Schlüssel abzulegen.

Ist der Füllgrad des Datenfeldes zu groß um eine Verschlüsselung mit den vorgenannten Kriterien durchführen zu können, wird das Datenfeld zunächst komprimiert. Führt auch die Komprimierung des Datenfeldes nicht zu einer hinreichend kleinen Feldgröße, erfolgt die Pseudonymisierung. Das Pseudonym muß so gewählt werden, daß die oben unter 2.) vorgegebene Bedingung hinsichtlich des Füllungsgrades des Datenfeldes erfüllt wird.

Ist der Füllgrad des Datenfeldes hinreichend gering, um eine Verschlüsselung des Datenfeldes zu ermöglichen, wird die Verschlüsselung vorgenommen. Dafür wird das Datenfeld zunächst bis zum maximal möglichen Füllgrad mit zufälligen Werten aufgefüllt.

Bei geringem Informationsgehalt des Datenfelds kann vor der Auffüllung eine Datenkomprimierung vorgenommen werden, um Isonomien besser auflösen zu können.

Anschließend wird die Verschlüsselung vorgenommen. Der verwendete Verschlüsselungsalgorithmus kann beliebig gewählt werden. Gängige Algorithmen sind z. B. IDEA (International Data Encryption Algorithm) oder DES (Data Encryption Standard).

Das verschlüsselte Datenfeld wird dann mit einem Start- und einem Stoppzeichen gekennzeichnet. Außerdem wird im Datenfeld an einer vorher definierten Position eine Information über den zur Verschlüsselung verwendeten Schlüssel abgelegt.

Das nachfolgende Beispiel soll das Verfahren veranschaulichen:

Die Datenfeldlänge beträgt 40 Zeichen. Inhalt des unverschlüsselten Datenfeldes ist der Name "Meier". Als Startzeichen dient "{", als Stoppzeichen "}". Das Datenfeld wird auf die volle Feldlänge aufgefüllt und mit Start- und Stoppzeichen versehen, also:

{Meier. . .}.

An das Verfahren werden die 40 Zeichen zwischen den Start- und Stoppzeichen übergeben. Die Verschlüsselung ergibt dann ein 40 Zeichen langes Datenfeld einschließlich Start- und Stoppzeichen, also z. B.:

{ch74nHhdjqa. . .yjas8}.

In den verschlüsselten Datenfeldern sind k Bits zur Kennzeichnung des verwendeten Schlüssels aus einem Schlüsselsatz vorgesehen. Somit ist es möglich, 2^k verschiedene Schlüssel darzustellen. Durch die Aufnahme von Zusatzinformationen in die verschlüsselten Datenfelder, wie z. B. Menge von Start- und von Stoppzeichen, Schlüsselbits und Informationen über den verwendeten Initialisierungssektor für den Verschlüsselungsalgorithmus ist eine Komprimie-

rung der zu verschlüsselnden Datenfelder notwendig.

In der beigefügten **Fig.** 2 ist die Ver- bzw. Entschlüsselung von Datenfeldern dargestellt. Die einzelnen Schritte werden nachfolgend näher erläutert.

Die Beschreibung des Verfahrens geht von den folgenden Voraussetzungen aus:

- Jedes Zeichen wird durch ein Byte dargestellt (z. B. ASCII- oder EBCDIC-Code). Vor der Ver- bzw. Entschlüsselung werden alle Zeichen eines Feldes in einen internen Zeichensatz (ASCII) umgewandelt und danach wieder entsprechend konvertiert.
- Die unterschiedlichen Parameter sind wie folgt festgelegt:
  1. einen Zeichensatz (z. B. 91 bestimmte Zeichen des EBCDIC-Codes);
  2. eine Menge der Startzeichen und Stoppzeichen für verschlüsselte Datenfelder, die nicht im Zeichensatz enthalten sind;
  3. ein Ersatzzeichen für nicht zum Zeichensatz gehörende Zeichen (ist Bestandteil des Zeichensatzes);
  4. ggf. notwendige Füllzeichen (ist Bestandteil des Zeichensatzes);
  5. Verfahrensparameter für die Kompression;
  6. Angaben darüber, wie bei nicht erfolgreicher Komprimierung das ursprüngliche Datenfeld nachverarbeitet werden soll;
  7. Angaben zur Darstellung von Bitfolgen als Folgen zulässiger Zeichen;
  8. Angaben darüber, welcher der Schlüssel aus dem Schlüsselsatz verwendet werden soll.

In Abhängigkeit von der Mächtigkeit des Zeichensatzes lassen sich einzelne Bitsegmente jeweils zu Zeichenfolgen einer bestimmten Länge umformen (zum Beispiel können bei einem Zeichensatz von 91 Zeichen je 13 Bit in je 2 Zeichen effektiv umgeformt werden). Optimal wäre eine "gemeinsame" Umformung der gesamten Bitfolge durch Betrachtung der Folge als Binärzahl und Darstellung dieser Zahl zur Basis b = Mächtigkeit des Zeichensatzes.

Im folgenden wird ein Verfahren zur effektiven Codierung einer möglichst großen Bitfolge in ein Datenfeld einer vorgegebenen Länge beschrieben, das für eine Implementierung auf Systemen mit 32-Bit-Prozessoren vorgesehen ist. Zunächst wird für einen gegebenen Zeichensatz vom Umfang b vor der Grundinitialisierung einmalig folgendes berechnet ("ln" bezeichnet hierbei den natürlichen Logarithmus):

- Bestimmung des Minimalwertes von x/y für ganzzahliges y von 1 bis 32 und ganzzahliges $x \geq y \cdot \ln(2)/\ln(b)$.
  Beispiel: Bei b = 91 erhält man ein Minimum bei x = 2 und y = 13.
- Für alle Werte x' von 1 bis x–1 wird das jeweilige ganzzahlige Maximum y'(x') mit $y'(x') \cdot \ln(2)\ln(b) \leq x'$ berechnet. Außerdem wird y'(0): = 0 gesetzt.
  Beispiel: Bei b = 91 und x = 2 erhält man y'(1) = 6.

Es läßt sich nun folgendermaßen eine Bitfolge in ein Datenfeld der Länge d umformen:

1. Umformung von je y Bit in je x Zeichen.
   Beispiel: Bei b = 91 werden je 13 Bit durch je 2 Zeichen dargestellt.
2. Falls die gegebene Datenfeldlänge d nicht durch x teilbar ist, dann werden y'(x') Bit in die restlichen x' Zeichen umgeformt. Im Beispiel werden noch 6 Bit durch ein Zeichen dargestellt.

Bei s die Anzahl der verwendeten Startzeichen in den verschlüsselten Datenfeldern und

$$L(d, b, s) = L = ((d\text{-}s\text{-}1)\,\mathrm{DIV}\,x) \cdot y + y'((d\text{-}s\text{-}1)\,\mathrm{MOD}\,x)$$

die Anzahl der Bits, die sich durch Anwendung des obigen Verfahrens in ein Datenfeld der Länge (d-s-1) umformen lassen. Der Wert (d-s-1) resultiert daraus, daß im verschlüsselten Datenfeld die Menge der Startzeichen der Länge s und das Stoppzeichen enthalten sein müssen.

Bei d = 30, b = 91 und s = 1 erhält man zum Beispiel $L = 14 \cdot 13 + 0 = 182$, bei d = 15, b = 91 und s = 3 ergibt sich $L = 5 \cdot 13 + y'(1) = 65 + 6 = 71$.

m = (L-k-Länge komprimierte Bitfolge) sei, die nach der Kompression noch zur Verfügung stehenden Bits, k Bits sind für die Nummer des verwendeten Schlüssels vorgesehen. Für die Kompression können die verschiedensten Methoden eingesetzt werden. In Abhängigkeit von dieser Zahl m wird festgelegt, wie der Initialisierungsvektor für die Verschlüsselung bereitgestellt und codiert wird.

Die geeignete Wahl des Initialisierungsvektors sorgt dafür, daß Isonomien aufgelöst werden. Es gibt hierfür prinzipiell die folgenden Möglichkeiten, die eingesetzt werden können:

- Verwendung von Zufallszahlen
- Verwendung von Zählern.

Zeitlich gestaffelt können verschiedene Schlüssel des aus k Schlüsseln bestehenden Schlüsselsatzes eingesetzt werden. Bei der Verschlüsselung ist festzulegen, welcher dieser Schlüssel verwendet werden soll. Die Schlüsselnummer wird durch k Bits kodiert.

Wenn die aus k Bits für die Nummer des Schlüssels, den Bits für die Codierung des Initialisierungsvektors und den Bits des komprimierten Datenfeldes bestehende Bitfolge kürzer als erforderlich sein sollte, d. h. kleiner als L ist, so wird sie am Ende mit Bits "0" aufgefüllt, bis die maximal zulässige Bitlänge L erreicht ist.

Verschlüsselt wird der komprimierte Datenfeldinhalt.

Die Verschlüsselung kann mit einem Blockverschlüsselungsalgorithmus erfolgen und dem gespeicherten geheimen Schlüssel im CBC-Modus, wobei der letzte Block der Länge j (falls diese kürzer als 64 Bit ist) im CFB-Modus verschlüsselt wird (siehe z. B. ISO/IEC 10116, Informations Technologie – Modes of Operation for ann-bit Block Cipher Algorithm, 1991).

Bei der Betrachtung wird davon ausgegangen, daß die typische Blocklänge von 64 verwendet wird. Eine Verallgemeinerung auf andere Blocklängen ist offensichtlich. Eine andere Variante, die sog. Stromverschlüsselungsalgorithmen, könnten direkt zur zeichenweisen Verschlüsselung eingesetzt werden.

Zur Bildung des verschlüsselten Datenfeldes wird schließlich die erhaltene Zeichenfolge zwischen der Menge Startzeichen und dem Stoppzeichen eingefügt.

Sobald im Datenstrom die Startzeichenfolge erkannt wird, werden die nachfolgenden Zeichen in einen internen Speicher gegeben, bis das Stoppzeichen erscheint.

Falls sich unter den nachfolgenden Zeichen die Startzeichenfolge befindet, wird der Prozeß der Einspeicherung abgebrochen und bei der neuen Startzeichenfolge begonnen. Falls nach einer vorgegebenen Maximallänge noch kein Stoppzeichen festgestellt wurde, wird der Prozeß ebenfalls abgebrochen und es wird erneut nach der nächsten Startzei-

chenfolge gesucht. Falls zwischen der Menge Startzeichen und dem Stoppzeichen weniger als eine vordefinierte untere Schranke Zeichen sind, wird die Einspeicherung ebenfalls abgebrochen.

Nicht jedes Datenfeld kann so stark komprimiert werden, daß die angestrebte Anzahl Bits für den Initialisierungsvektor zur Verfügung steht. Je kürzer die Datensatzlänge ist, desto schlechter ist die Komprimierung, mit der Konsequenz, daß weniger Bits für den Initialisierungsvektor zur Verfügung stehen und somit weniger Möglichkeiten verschiedene Chiffrate für ein Datenfeld zu erzeugen.

In einem solchen Fall gibt es prinzipiell die folgenden drei Möglichkeiten fortzufahren:

1. Kürzung des Datenfeldes bis eine ausreichende Komprimierung erreicht werden kann. Dies ist aber zwangsläufig mit Informationsverlust verbunden. 2. Das betroffene Datenfeldes wird nicht verschlüsselt, es wird somit in Klartext bleiben. Dies kann möglicherweise akzeptabel sein, falls dies im Verhältnis zu der gesamten Menge zu verschlüsselten Datenfelder sehr selten vorkommt.
3. Verwendung des Pseudonymisierungsansatzes, dieser wird im folgenden beschrieben.

Bei vorgegebener fester Feldlänge, kann der Fall eintreten, daß keine ausreichende Komprimierung der Datensätze erreicht werden kann. Ist eine Kürzung oder das Weiterleiten in Klartext nicht akzeptabel, so kann die vollständige "Verschleierung" aller ausgewählten Datensätze, durch den Pseudonymisierungsansatz realisiert werden.

Analog zu einem Alias, erfolgt eine Verknüpfung von Datenfeldern und Pseudonymen und vice versa. Die Informationen werden in einer Tabelle gehalten.

Leutheusser-Schnarrenberger ↔ X1BXE. . .H
Garmisch-Partenkirchen ↔ X2BXD9. . .Z

Falls die Pseudonymisierung an mehreren räumlich getrennten Orten notwendig ist, müssen die an allen Standorten vergebenen Pseudonyme an allen anderen Standorten vorgehalten werden (Replikation). Dies bedeutet zusätzliche Kommunikationskosten. Es sind zusätzliche Maßnahmen zur Sicherung der Übertragung notwendig.

Die Speicherung von verschlüsselten Datenfeldern kann über längere Zeiträume, z. B. 5–15 Jahre, erfolgen. Die zeitlich gestaffelte Verwendung von mehr als einem Schlüssel ist aus den folgenden Gründen ratsam:

– Wird der Schlüssel bekannt, ist die gesamte Menge der verschlüsselten Datenfelder als offengelegt zu betrachten.
– Die einem Krypto-Analysten zur Verfügung stehende Menge von verschlüsselten Datenfeldern, ist wesentlich geringer, wenn mehrere Schlüssel verwendet werden.

Deshalb sieht das Verfahren pro Menge von Datenbanknutzern, die kooperieren, k Schlüssel vor.

In einem Trust Center (vertrauenswürdige dritte Instanz), welches das notwendige technische und organisatorische Umfeld stellt, können die Schlüssel generiert werden. Verschiedene Mengen von Datenbanknutzern, die nicht miteinander kooperieren, sollten verschiedene Mengen von Schlüsseln haben, die keinerlei Abhängigkeit von einander haben. So ist ausgeschlossen, daß eine Menge von Datenbanknutzern auf Datenbankinformationen der anderen Menge von Datenbanknutzern zugreifen kann. Das Key Management besteht aus folgenden Funktionen:

1. Schlüsselerzeugung
Erzeugung eines Schlüsselpaktets aus k Schlüsseln. Hierfür eignet sich besonders ein Hardware Zufallszahlengenerator. Im Nachgang der Schlüsselerzeugung können die generierten Schlüssel auf ein Schlüsselaufbewahrungsmedium, z. B. eine Chip- oder PCMCIA-Karte, gespeichert werden. Diese Medien können so konfiguriert werden, daß sie die kryptographischen Berechnungen selbst ausführen oder Schlüssel erst nach vorheriger Authentisierung herausgeben.
2. Schlüsselverteilung
Vom Ort der Schlüsselgenerierung können die Schlüssel auf einem Schlüsselaufbewahrungsmedium zum Einsatzort (Endgerät) oder zur sicheren Aufbewahrung (Backup) transportiert werden.
3. Schlüssel in Endgeräte einbringen
Ein Endgerät zeichnet sich dadurch aus, daß es die notwendigen Ver- bzw. Entschlüsselungsprozesse ausführen kann. Ein solches Gerät kann eine speziell entwickelte Hardware oder ein PC sein. Die Schlüssel können aus dem Schlüsselaufbewahrungsmedium nach vorheriger Authentisierung in ein Endgerät geladen werden oder das Endgerät kann Aufträge zur Ver- und Entschlüsselung entgegennehmen. Der letzte Fall setzt eine entsprechende Ressource des Schlüsselaufbewahrungsmediums voraus, hat aber der Vorteil, daß die Schlüssel nie das Schlüsselaufbewahrungsmedium verlassen.
4. Schlüssel vernichten
Falls ein kooperierende Menge von Datenbanknutzern ein Schlüsselpaket aus k Schlüsseln nicht mehr benötigt, ist es möglich, die Schlüssel durch geeignete Maßnahmen zu vernichten, z. B. durch Vernichtung des Schlüsselaufbewahrungsmediums und Löschen des, Schlüsselpakets aus den entsprechenden Endgeräten, falls vorhanden.

Patentansprüche

1. Verfahren zur Anonymisierung sensibler Daten innerhalb eines Datenstroms mit den folgenden Schritten:
   a) Anonymisierung des sensiblen Datenfeldes.
   b) Kennzeichnung des anonymisierten sensiblen Datenfeldes innerhalb des Datenstroms durch Start- und Stoppzeichen.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß vor der Anonymisierung eine Komprimierung des sensiblen Datenfeldes stattfindet.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß das sensible Datenfeld vor der Anonymisierung durch Füllzeichen aufgefüllt wird.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die zu anonymisierenden Daten pseudonymisiert werden.
5. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die zu anonymisierenden Daten verschlüsselt werden.
6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß sensible Datenfelder vor der Verschlüsselung zumindest teilweise mit zufälligen Werten aufgefüllt werden.
7. Verfahren nach Anspruch 5 oder 6, dadurch gekennzeichnet, daß im verschlüsselten Datenfeld Informationen über den zur Verschlüsselung verwendeten Schlüs-

sel abgelegt werden.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß das sensible Datenfeld eine feste Feldlänge aufweist.

Hierzu 4 Seite(n) Zeichnungen

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

Nummer: DE 199 11 176 A1
Int. Cl.[7]: H 04 L 9/00
Offenlegungstag: 21. September 2000

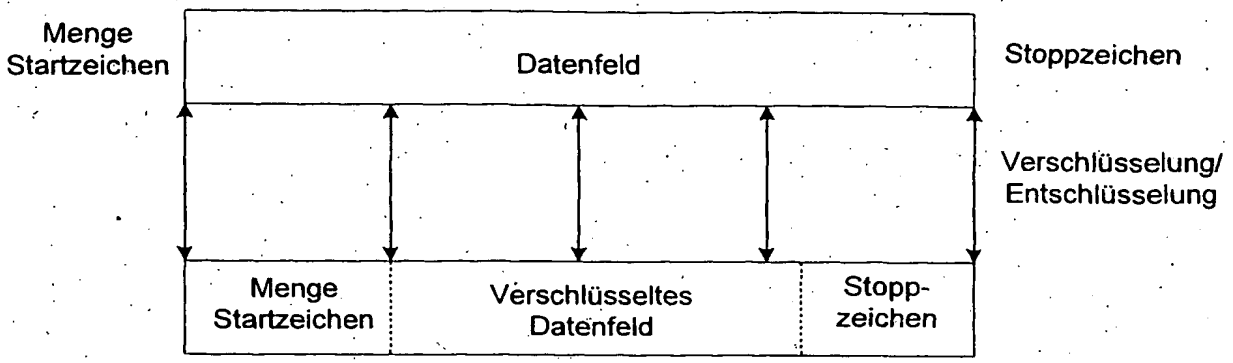

Fig. 1

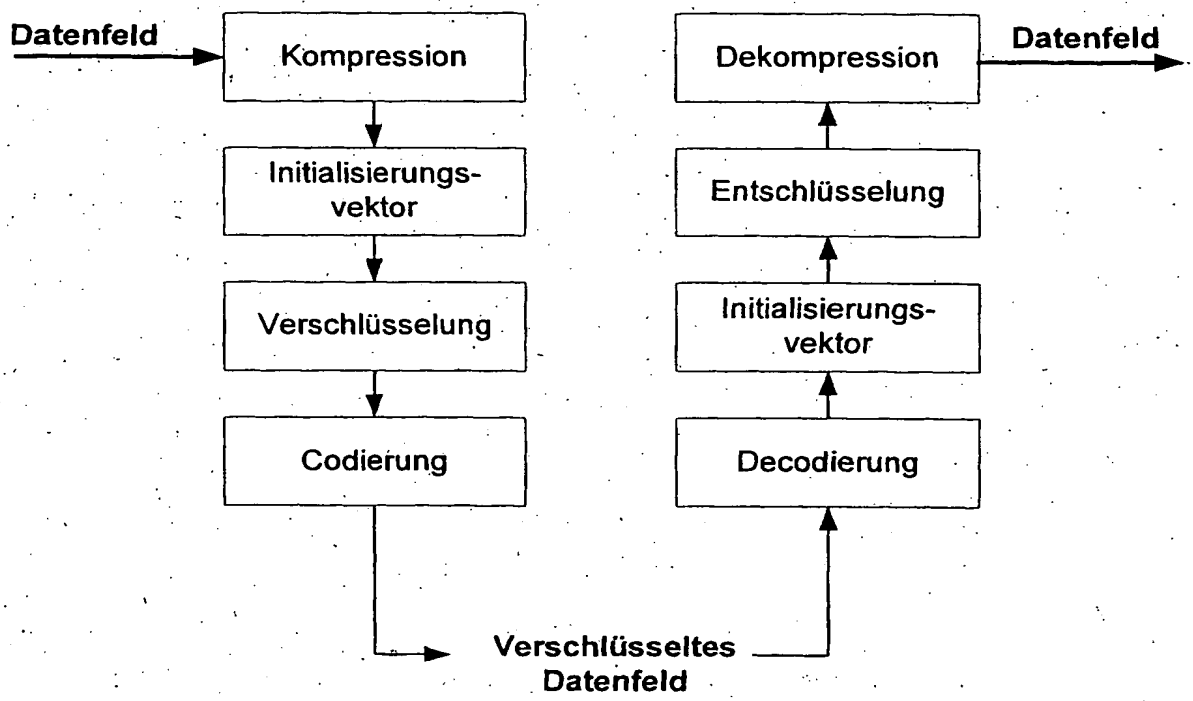

Fig. 2

Nummer: DE 199 11 176 A1
Int. Cl.[7]: H 04 L 9/00
Offenlegungstag: 21. September 2000

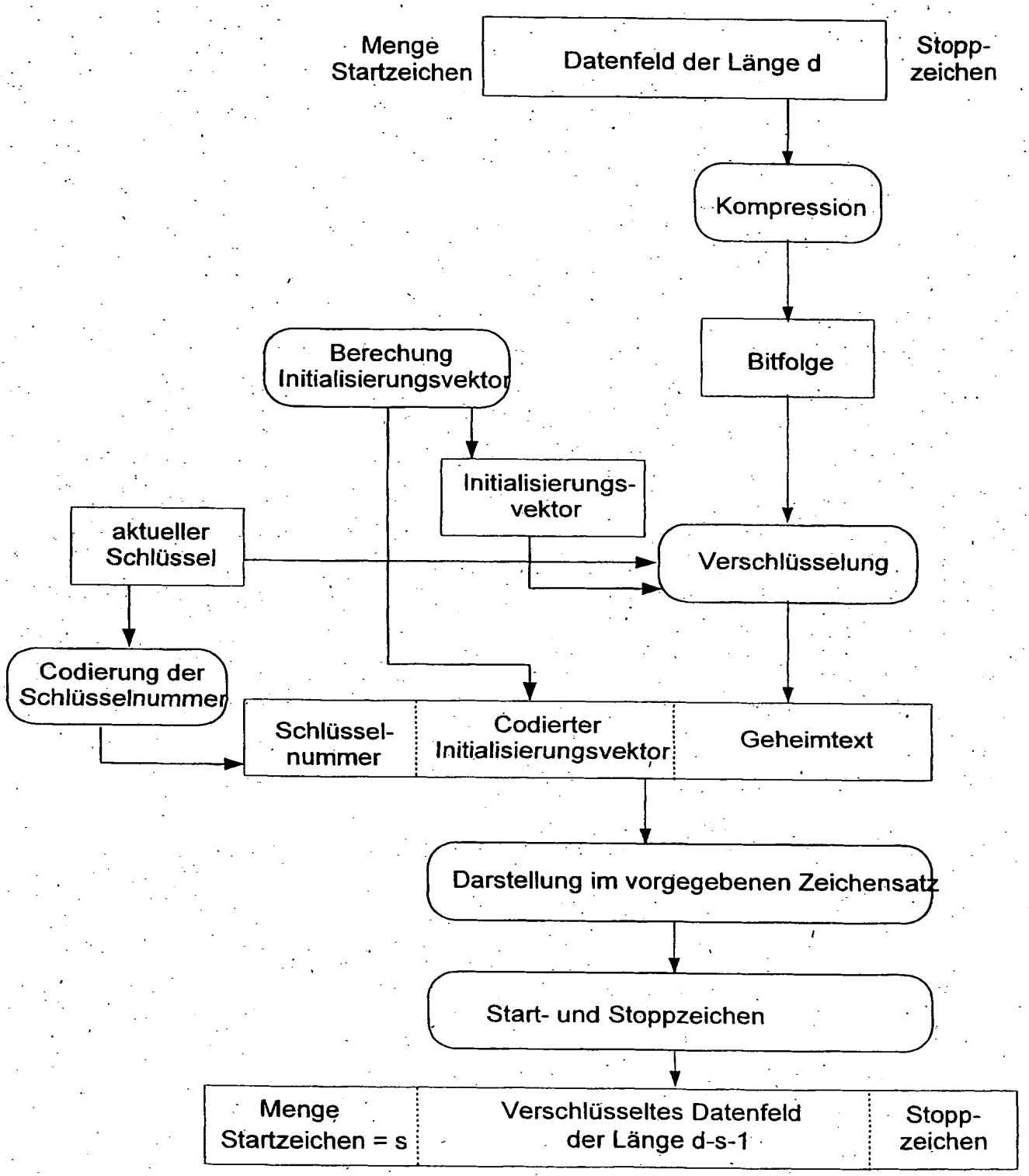

Fig. 3

Nummer: DE 199 11 176 A1
Int. Cl.[7]: H 04 L 9/00
Offenlegungstag: 21. September 2000

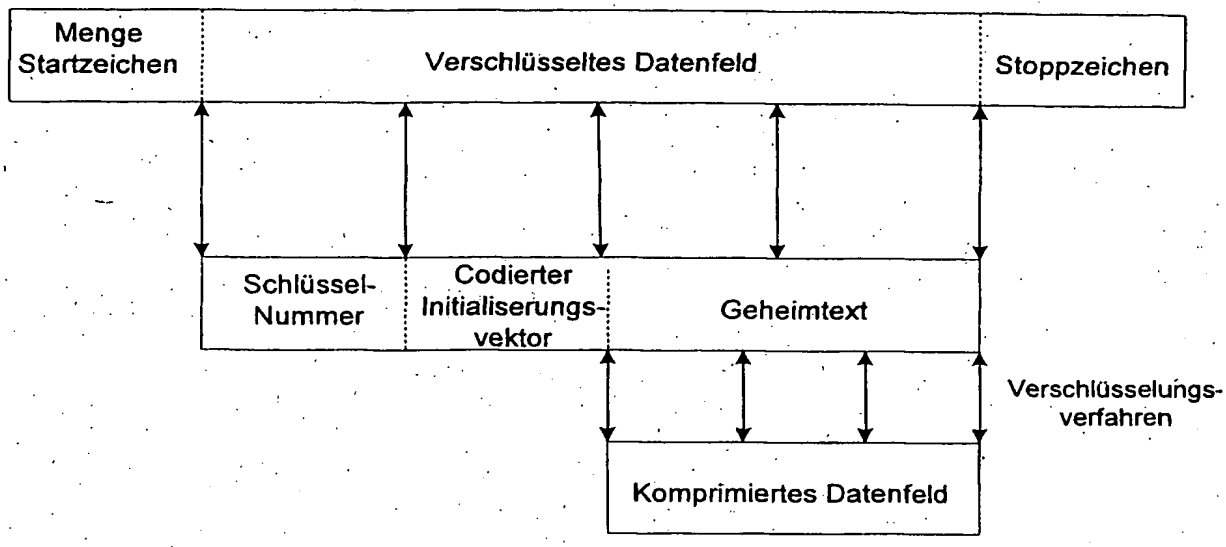

Fig. 4

Nummer: DE 199 11 176 A1
Int. Cl.[7]: H 04 L 9/00
Offenlegungstag: 21. September 2000

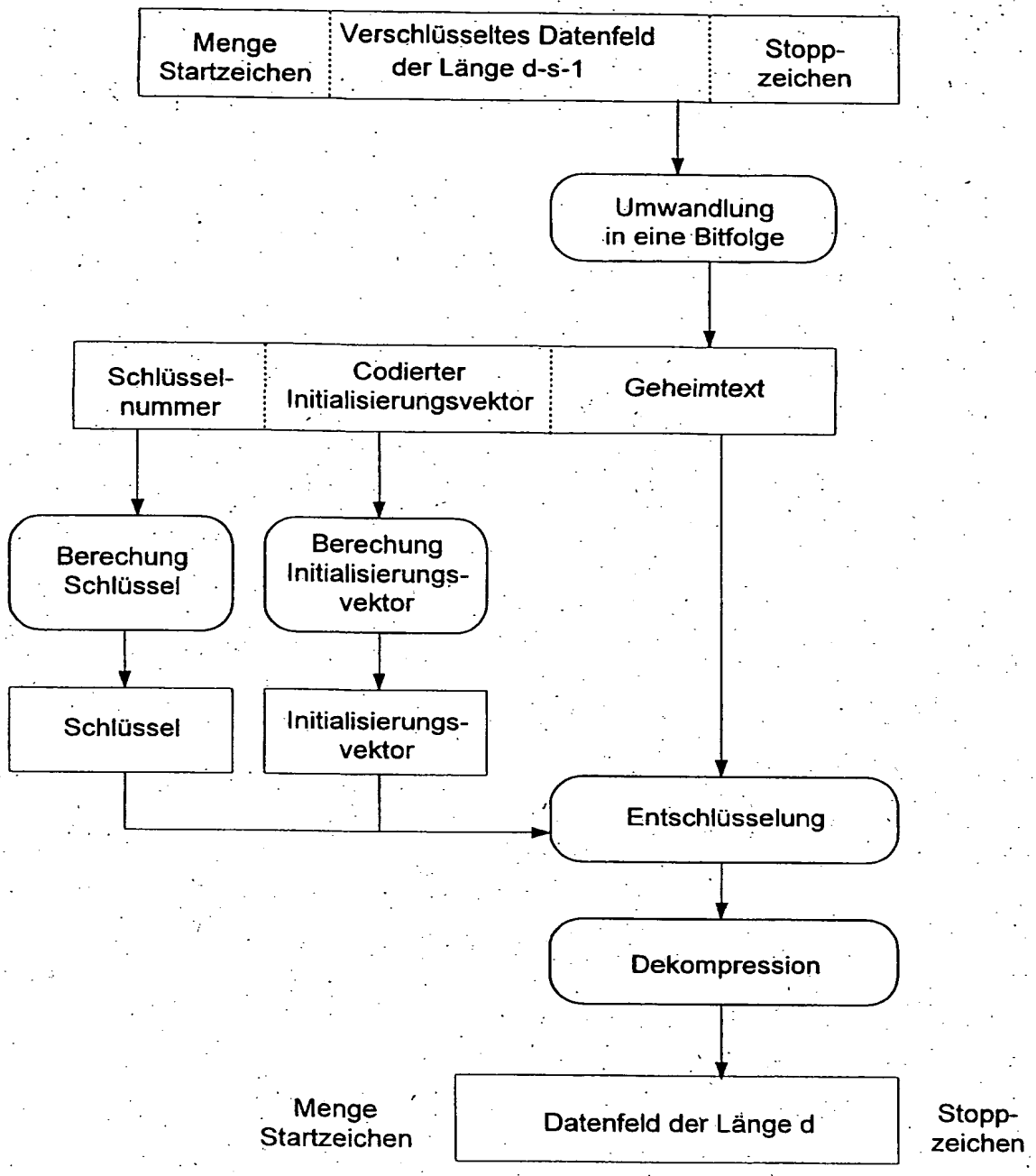

Fig. 5